

REMARKS

Claims 1, 2, 4-7, 13, 14, 16, 20, 21 and 23 were allowed. Claims 8, 17 and 24 were rejected. And claims 9-11, 18-19 and 25-26 were objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

In response, Applicants thank the Examiner for the indication of allowable subject matter. However, for reasons set forth below, Applicants respectfully submit the rejected claims are also allowable. Therefore, reconsideration of the application is respectfully requested.

CLAIM REJECTIONS – 35 U.S.C. §102

In “Claim Rejections – 35 USC § 102” item 3 on page 2 of the above-identified Office Action, claims 8, 17 and 24 have been rejected as being anticipated by U.S. Patent No. 5,680,458 (hereinafter Spelman) under 35 U.S.C. § 102(b).

Independent claim 8 recites a method comprising:

“producing a document comprising an identification of a software module binary and a list of compromised keys; and

digitally signing the document using a key presented by or read from the document and traceable to one key of a set of keys, wherein the set of keys is embedded in the software module binary, the set of keys having been compiled and linked with a software module to generate the software module binary.”

Spelman recites a method of recovering from a compromise of a root key which is the private key of a first public key- private key pair. In particular, according to col.4 lines 15-20, Spelman involves using an in-band channel to distribute a key compromise emergency message, and using an out-of band channel to publish a verification code to verify the authenticity of the emergency message.

The Examiner cited col. 4 lines 34-46 of Spelman to read on “producing a document comprising an identification of a software module binary and a list of compromised keys” in claim 8. However, Applicants respectfully disagree. Col. 4 lines 34-46 of Spelman discloses that an emergency message 10 includes a message identifier 12, a serial number 14 identifying the compromised root key, and a replacement key 16, etc. Without discussing that if the

emergency message 10 in Spelman can be read as the document in claim 8 or if the serial number 14 in the emergency message of Spelman can be read as the list of compromised keys in claim 8, Applicants submit that Spelman fails to disclose the software module binary and consequently fails to disclose an identification of the software module binary in claim 8. According to col. 4, lines 37-38 of Spelman, the identification of message 14 identifies the message as an emergency message, but cannot be read as the identification of a software module binary. Otherwise, the emergency message 10 may have to be read as the software module binary, and in that case nothing can be read as the document in claim 8. So, Applicants submit that Spelman fails to teach “producing a document comprising an identification of a software module binary and a list of compromised keys” in claim 8 in either way.

Also, the Examiner cited col.5, lines 9-16 to read on “digitally signing the document using a key presented by or read from the document and traceable to one key of a set of keys, wherein the set of keys is embedded in the software module binary” and col. 6, lines 33-46 to read on “the set of keys having been compiled and linked with a software module to generate the software module binary” in claim 8. Col.5, lines 9-16 discloses of Spelman discloses that a central authority uses the compromised root key to generate the digital signature. Col. 6, lines 33-46 discloses that the user verifies the digital signature by applying a public key algorithm using the compromised root key. However, neither these cited portions nor the other parts of Spelman disclose anything that can be deemed as the software module binary in claim 8. Thus, Applicants submit that Spelman fails to teach these two elements, both of which have recitation of the software module binary claim 8.

For all the reasons above, claim 8 is patentable over Spelman under 35 U.S.C. § 102(b). Thus, Applicant respectfully requests reconsideration and withdrawal of the rejection to claim 8.

Amended, independent claims 17 and 24 contain generally similar subject matter to that of claim 8. Claims 9-11, 18-19 and 25-26 depend from claim 8, 17 or 24, incorporating their recitations respectively. Thus, due to at least the reasons stated above, claims 9-11, 17-19 and 24-26 are patentable over Spelman under 35 U.S.C. § 102(b).

CONCLUSION

In light of the above amendments and remarks, all pending claims are in condition for allowance. Early issuance of Notice of Allowance is respectfully requested. If the Examiner has any questions, the Examiner is invited to contact the undersigned at 206-381-8819.

The Commissioner is hereby authorized to charge shortages or credit overpayments to Deposit Account No. 500393.

Respectfully submitted,
SCHWABE, WILLIAMSON & WYATT, P.C.

Dated: November 24, 2008

/Al AuYeung/
Al AuYeung
Reg. No. 35,432

Pacwest Center, Suite 1900
1211 SW Fifth Avenue
Portland, Oregon 97204
Telephone: (503)222-9981